On the Ranks of CM Types

Liem Mai

A Thesis

in

The Department

of

Mathematics

Presented in Partial Fulfillment of the Requirements
for the degree of Master of Science at
Concordia University
Montréal, Québec, Canada

August 1987

ISBN 0-315-37096-3

ABSTRACT

On the Ranks of CM Types

Liem Mai

This thesis studies the ranks of CM types (K,S). By using the characters of the corresponding Galois group, some properties and lower bounds for the ranks are given in the case that K is a cyclotomic field and especially S is a CM type of a Fermat curve. Some algorithms are presented, together with their analysis, to find the ranks of CM types.

ACKNOWLEDGEMENTS

I wish to express my great gratitude to my supervisor, Prof. V.K. Murty for his superb guidance, encouragement and support in the preparation and composition of this thesis. I really feel fortunate to have had Dr. V.K. Murty as my thesis supervisor.

I am also grateful to Profs. Kisilevsky, Raphael and especially Prof. Malik for various supports, advices and discussions which make the completion of this thesis possible.

I wish to thank the Natural Science and Engineering Research Council (NSERC) for providing me a postgraduate scholarship.

Last, but not least, I wish to express my special thanks to my parents and siblings for their continuous encouragement and moral support during my studies.

TABLE OF CONTENTS

Chapter 1

CM fields and CM types

1.1 CM fields

Let $K \subset \mathbb{C}$ be a number field.

By a totally real field, we mean a field $K_1 \subset \mathbb{C}$ such that for any embedding $K_1 \hookrightarrow \mathbb{C}$, the image is contained in $\mathbb{R}$. By a totally imaginary field we mean a field $K_2 \subset \mathbb{C}$ such that for any embedding $K_2 \hookrightarrow \mathbb{C}$, the image is not contained in $\mathbb{R}$.

K is said to be a CM field (complex multiplication field) if it is a totally imaginary quadratic extension of a totally real field K^+.

Example 1 : Let p be a rational prime and ξ_p be a primitive p^{th} root of unity. Then $K = \mathbb{Q}(\xi_p)$ is a CM field, in which $K^+ = \mathbb{Q}(\xi_p + \xi_p^{-1})$.

Indeed, we have the following well-known criterion for a field to be a CM field.

Proposition 1 : Let K be a number field and $\rho : \mathbb{C} \to \mathbb{C}$ in which $\rho\,(a+bi) = a-bi$. Then K is a CM field if and only if $\rho|_K$ is a non trivial automorphism of K commuting with every embedding of K into $\mathbb{C}$.

1.2 CM Types :

Let K be a CM field of degree $[K:\mathbb{Q}] = 2m$. By a CM type of K we mean a set S of embeddings $\psi_1,\ldots,\psi_m$ of K in $\mathbb{C}$ such that the set of all embeddings of K in $\mathbb{C}$ consists of $\psi_1,\ldots,\psi_m,\psi_1\rho,\ldots,\psi_m\rho$.

Example 2 : Let K be a finite Galois extension of $\mathbb{Q}$ with Galois group $Gal(K/\mathbb{Q})=G$. Then a CM type S is a set of coset representatives for $\{ 1, \rho \}$.
Usually, we denote a CM type as (K,S) or simply S if K is fixed.

Now let (K,S) be a CM type and let F be a finite extension of K. Let S_F be the inverse image of S on F, i.e the set of all embeddings φ of F into $\mathbb{C}$ which induce some elements ψ_i of S on K. If $S_F = \{ \varphi_1,...,\varphi_n \}$ then $[F:\mathbb{Q}] = 2n$. In this case, we say that (F,S_F) is the type lifted from the CM type (K,S).

Proposition 2 : Suppose F is Galois over $\mathbb{Q}$ with $Gal(F/\mathbb{Q}) = G$. Let $H = H(S_F) = \{ \sigma \in G : \sigma S_F = S_F \}$. Let K_o be the fixed subfield of H and S_o be the set of all embeddings of K_o into $\mathbb{C}$, induced by those of S_F on K_o.

Then K_o is a CM field, (K_o,S_o) is a CM type and (F,S) is lifted from (K_o,S_o). Furthermore, $K_o \subset K$ and K_o is the smallest subfield of F having this property.
Proof : see Lang [9].

A type (K,S) is called simple if it is not lifted from a CM type of a proper subfield.

If F is not Galois over $\mathbb{Q}$ then we can consider the normal closure L of F. L also contains K and the above results can be applied for L. Therefore we can assume that F is Galois over $\mathbb{Q}$.

1.3 Reflex of a CM type

Let (K,S) be a CM type and L be the normal closure of K, with

Galois group $G = \mathrm{Gal}(L/\mathbb{Q})$. Let H be the subgroup of G defining K (i.e. $K = L^H$) . Now define $\tilde{S} = \{ g \in G : Hg \in S \}$. By [14], (K,S) is simple if and only if $H = \{ g \in G : g\tilde{S} = \tilde{S} \}$. Set $H' = \{ g \in S : \tilde{S}g = \tilde{S} \}$. It is easy to check that H' is a subgroup of G. Moreover,

Proposition 3 : Let $\tilde{R} = \tilde{S}^{-1}$. then $H' = \{ g \in G : g\tilde{R} = \tilde{R} \}$

Proof : If $g \in H'$ then for any $\tilde{r} \in \tilde{R}$, we have

$$\tilde{r}_2^{-1} g = \tilde{r}^{-1} \text{ for some } \tilde{r}_2 \in \tilde{R}.$$

$$\Rightarrow \tilde{r}_2^{-1} = \tilde{r}^{-1} g^{-1}$$

$$\Rightarrow \tilde{r}_2 = g\tilde{r}.$$

Similarly $\{ g \in G : g\tilde{R} = \tilde{R} \} \subset H'$.

Now let $K' = L^{H'}$ and $R' = \pi(\tilde{R})$ in which π is the projection $\pi : G \to G/H'$ (Here, G/H' denote the left coset space mod H') . (K',R') is called the reflex of the CM type (K,S) . Note that in the case K is Galois over $\mathbb{Q}$, $G = \mathrm{Gal}(K/\mathbb{Q})$ and $\tilde{S} = S$, $\tilde{R} = R$

In [14] Shimura and Taniyama show that the reflex field K' is the field generated over $\mathbb{Q}$ by all elements $\{ \mathrm{tr}S(x) = \sum_{\psi_i \in S} \psi_i(x) \ / \ x \in F \}$.

Proposition 4 : Suppose that $(K;S)$ is a CM type, in which K is Galois and Abelian over $\mathbb{Q}$. If S is simple, R is also simple.

Proof :

Suppose that S is simple and R is not simple. Then there exists $g \in G$, $g \neq id$ such that for all $r \in R$, there exists $r_2 \in R$: $rg = r_2$. Then $g^{-1}s = s_2$. But then S is not simple : contradiction.

Theorem 1 : Let (K,S) be a CM type. Then

i) K' is a CM field.

ii) (K',R') is a simple CM type. Thus K' is the smallest field from which R' is lifted.

iii) If (K,S) is simple, the reflex of (K',R') is also simple and equal to (K,S).

Proof : see Shimura and Taniyama [14].

1.4 Rank of a CM type

Let (K,S) be a simple CM type and (K',R') be its reflex CM type. Denote by X(K) the free $\mathbb{Z}$-module spanned by $\{ \sigma \mid \sigma : K \hookrightarrow \mathbb{C} \}$ and similarly X(K'). A typical element of X(K) has the form $\sum_{\sigma:K\hookrightarrow\mathbb{C}} n_\sigma[\sigma]$, $n_\sigma \in \mathbb{Z}$ (a formal sum). Suppose that K is Galois over $\mathbb{Q}$ then $K' \subset K$. Define a $\mathbb{Z}$-module homomorphism :

$$\phi : X(K) \to X(K')$$

$$[\sigma] \to \sum_{r'\in R'} [\sigma r'|_{K'}]$$

Note that ϕ is well defined since if σ is an automorphism of K into $\mathbb{C}$, so is $\sigma r'$ and then we can consider $\sigma r'|_{K'}$ as an isomorphism of K' into $\mathbb{C}$, in which $r' \in rH'$ (note that $K' = K^{H'}$) . If we choose another representation $r'' \in rH'$ then for any $k' \in K'$:

$$\sigma r''(k') = \sigma r'h'(k') = \sigma r'(k')$$

Obviously, ϕ is an $\mathbb{Z}$-module homomorphism.

Therefore $\mathrm{Im}\phi$ is a $\mathbb{Z}$-module and its rank over $\mathbb{Z}$ is called the rank of the CM type (K,S).

Proposition 5 (Kubota) : Let (K,S) be a CM type and (K',R') be its reflex CM type. Then

$$\text{rank } (K,S) = \text{rank } (K',R')$$

Proof : see Kubota [8].

1.5 Connection with Abelian varieties

The rank arises naturally in the study of Abelian varieties with complex multiplication. We briefly explain this here . (We shall not use the contents of this section in the remainder of the thesis).

Let k be a number field and let E be an elliptic curve defined over k with complex multiplication by an order $\mathcal{O}$ in an imaginary quadratic field F (i.e $\mathcal{O}$ is a subring of F and also a $\mathbb{Z}$-module of rank 2). Then for any rational prime ℓ and for any $n \in \mathbb{Z}$, $n \geq 1$, it is well-known that :

$$(\ell^n)^2 \ll [k(E[\ell^n]):k] \ll (\ell^n)^2$$

here $E[\ell^n]$ is the group of points in $E(\bar{k})$ of order dividing ℓ^n, $k(E[\ell^n])$ is the field obtained by adjoining to k the coordinates of all points in $E[\ell^n]$ and the implied constants depend only on E, k and F (but not on ℓ and n).

More generally, let A be an Abelian variety defined over a number field k . We say that A is of CM type if there exists a commutative semisimple algebra F over $\mathbb{Q}$ such that $F \hookrightarrow \mathrm{End}(A) \otimes_{\mathbb{Z}} \mathbb{Q}$ and $\dim_{\mathbb{Q}} F = 2 \dim A$. There is an integer $r \geq 1$, such that for any rational prime ℓ and for any $n \in \mathbb{Z}$, $n \geq 1$:

$$(\ell^n)^r \ll [k(A[\ell^n]):k] \ll (\ell^n)^r$$

in which the implied constants depend only on A, k and F (but not on ℓ and n) .

By Shimura and Taniyama [14], r is the rank of the CM type of A.

1.6 Bounds for the rank

Can we say anything about the rank of a simple CM type (K,S) in which K is assumed to be Galois over $\mathbb{Q}$, without loss of generality and $\mathrm{Gal}(K/\mathbb{Q}) = G$?

Proposition 6 : If (K,S) is a simple CM type, rank (K,S) $\leq \frac{|G|}{2} + 1$

Proof: If $\rho \notin S$ then we claim that $\{ \phi(\sigma) : \sigma \in S \text{ or } \sigma = \rho \}$ spans $\mathrm{Im}\phi$.

Indeed for any $\sigma \in S$:

$$\begin{aligned} \phi[\rho\sigma] + \phi[\sigma] &= \sum_{r' \in R'} [r'\sigma] + \sum_{r' \in R'} [r'\rho\sigma] \\ &= \sum_{r' \in G \backslash H'} [r'\sigma] . \end{aligned}$$

Similarly

$$\phi[\mathrm{id}] + \phi[\rho] = \sum_{r' \in G \backslash H'} [r'\sigma]$$

Therefore

$$\phi[\rho\sigma] = \phi[\mathrm{id}] + \phi[\rho] - \phi[\sigma]$$

In other words $\{ \phi[\sigma] : \sigma \in S \text{ or } \sigma = \rho \}$ spans $\mathrm{Im}\phi$.

If $\rho \in S$ then $\{ \phi[\sigma] : \sigma \in S \text{ or } \sigma = \mathrm{id} \}$ spans $\mathrm{Im}\phi$.

In the case rank(K,S) $= \frac{|G|}{2} + 1$, we say that (K,S) is nondegenerate.

Theorem 2 (Ribet) : If (K,S) is a simple CM type and $[K:\mathbb{Q}] = 2d$. Then

$$\text{rank } (K,S) \geq \log_2(4d) = 2 + \log_2 d.$$

Proof : see Ribet [12].

Indeed theorem 2 can be refined by :

Theorem 3 (Murty) : Let r = rank (K,S), in which (K,S) is a simple CM type , [K:Q] = 2d . Then

$$r \geq \max \{ \frac{(p-1)^2\alpha}{p} , \text{ p odd prime and } p^{\alpha} \| d \}.$$

At first we need a lemma .

Lemma 1 : Consider $\phi : X(K) \to X(K')$

$$[\sigma] \to \sum_{r' \in R'} [\sigma r'|_{K'}]$$

Let $Y = \mathrm{Im}\phi$, $G = \mathrm{Gal}(K/Q)$ then

$$\mathcal{T} : G \to GL(Y)$$

$$g \to \mathcal{T}(g) = \mathcal{T}_g : Y \to Y$$

$$\phi[\sigma] \to \phi[g\sigma]$$

is an injective group homomorphism.

Proof of lemma 1 :

Observe that :

$$\mathcal{T}(g) = \mathcal{T}_g : Y \to Y$$

is well defined (note that $\{ \phi[\sigma] : \sigma \in G \}$ is not a basis for $\mathrm{Im}\phi$) . Given $\sum_{\sigma \in G} n_\sigma \phi[\sigma] = 0$, we claim that $\mathcal{T}_g(\sum_{\sigma \in G} n_\sigma \phi[\sigma]) = \sum_{\sigma \in G} n_\sigma \phi[g\sigma] = \sum_{\sigma \in G} \sum_{r' \in R'} n_\sigma [g\sigma r'|_{K'}] = 0.$

Indeed $\sum_{\sigma \in G} n_\sigma \phi[\sigma] = 0 \Rightarrow \sum_{\sigma \in G} n_{g\sigma} \phi[g\sigma] = 0$ and hence

$$\sum_{\sigma \in G} n_{g\sigma} \sum_{r' \in R'} [g\sigma r'] = 0 \qquad (*)$$

As the coefficient of [t] in (*) is $\sum_{r' \in R'} n_{tr'^{-1}}$ (since $g\sigma r' = t$ then $g\sigma$

$= tr'^{-1}$), hence

$$\sum_{r'\in R'} n_{tr'^{-1}} = 0$$

for all $t\in G$.

In particular, replacing t by $g^{-1}t$, we see that

$$\sum_{r'\in R'} n_{g^{-1}tr'^{-1}} = 0$$

But this is exactly the coefficient of $[t]$ in

$$\sum_{\sigma\in G}\sum_{r'\in R'} n_\sigma [g\sigma r']$$

Therefore $\mathcal{T}_g$ is well defined .

Next, $Y = \operatorname{Im}\phi$ is a submodule of $X(K)$ and $X(K)$ is a free $\mathbb{Z}$-module , hence Y is also a free $\mathbb{Z}$-module.

Now, $\mathcal{T}_g$ is onto for all $g\in G$ since for any $\phi[\sigma]\in Y$, we have:

$$\mathcal{T}_g(\phi[g^{-1}\sigma]) = \phi[\sigma]$$

Also, $\mathcal{T}_g$ is obviously 1-1 since $\mathcal{T}_g$ is an epimorphism of a $\mathbb{Z}$-module Y of finite rank, hence is also a monomorphism.

Now, it can be easily checked that $\mathcal{T} : G \to GL(Y)$ is a group homomorphism. Moreover suppose $\mathcal{T}_{g_1} = \mathcal{T}_{g_2}$. Then for all $\sigma\in G$, $\phi[g_1\sigma] = \phi[g_2\sigma]$. This implies that for any $r_1'\in R'$, there exists $r_2'\in R'$ such that $g_1\sigma r_1' = g_2\sigma r_2'$.

That is

$$\sigma^{-1}g_2^{-1}g_1\sigma R' \subset R'$$

but by theorem 1 , R' is a simple CM type and so $\sigma^{-1}g_2^{-1}g_1\sigma = \mathrm{id}$, ie. $g_2 = g_1$.

<u>Proof of theorem 3</u>

By lemma 1, we have an embedding $\mathcal{T} : G \hookrightarrow GL(Y)$. Since Y is a free $\mathbb{Z}$-module, $Y \simeq \mathbb{Z}^r$, in which r = rank Imϕ , then GL(Y) $\simeq GL(\mathbb{Z}^r) \simeq GL_r(\mathbb{Z})$.

Let q be a large rational prime, then $\mathcal{T}$ induces an embedding $\mathcal{T}_q$:

$$\begin{array}{ccc} G & \xrightarrow{\tau} & GL_r(\mathbb{Z}) \\ & \underset{\tau_q}{\searrow} & \downarrow \\ & & GL_r(\mathbb{Z}/q\mathbb{Z}) \end{array}$$

In particular d divides $|GL_r(\mathbb{Z}/q\mathbb{Z})|$. (*)

Note that $|GL_r(\mathbb{Z}/q\mathbb{Z})| = (q^r - 1)(q^r - q)\ldots(q^r - q^{r-1})$

$$= q^{r(r-1)/2}(q^r - 1)(q^{r-1} - 1)\ldots(q-1)$$

Now let $p^\alpha \| d = \frac{1}{2}[K:\mathbb{Q}]$, $p \neq 2$ and let q be a primitive root mod p^α. From (*)

$$\alpha \leq \text{ord}_p(|GL_r(\mathbb{Z}/q\mathbb{Z})|) = \sum_{i=1}^{r} \text{ord}_p(q^i - 1).$$

By our choice of q:

$$\begin{aligned} \text{ord}_p(q^i - 1) &= 0 \quad \text{if } (p-1) \nmid i \\ &= j+1 \quad \text{if } i = i_o p^j(p-1), \text{ and } (i_o, p) = 1 \end{aligned}$$

Let $\omega = \lfloor r/(p-1) \rfloor$, we have:

$$\begin{aligned} \alpha &\leq \sum_{j=1}^{\omega} \text{ord}_p(q^{j(p-1)} - 1) \\ &= \omega + \lfloor \omega/p \rfloor + \lfloor \omega/p^2 \rfloor + \ldots \\ &\leq \omega\,(1 + (1/p) + (1/p^2) + \ldots) \\ &= \frac{\omega}{1-(1/p)} = \frac{p\omega}{p-1} \leq pr/(p-1)^2 \end{aligned}$$

Therefore $r \geq \frac{(p-1)^2\alpha}{p}$ for all odd primes p, such that $p^\alpha \| d$.

Chapter 2

CM types of a cyclotomic field

In this chapter we consider the case K is a cyclotomic field $\mathbb{Q}(\xi_p)$, in which p is a prime. Then K is Galois over $\mathbb{Q}$, with $G = \mathrm{Gal}(K/\mathbb{Q}) \simeq (\mathbb{Z}/p\mathbb{Z})^* = \{ r^k : k = 0, 1, \ldots, p-2 \}$, a cyclic group with generator r, and $K^+ = \mathbb{Q}(\xi_p + \xi_p^{-1})$. Note that ρ is identified with $-1 = r^{(p-1)/2}$. At first we study the structure of simple CM types of K.

2.1 Simple CM types

Let S be a CM type in K. If S is simple then $H = \{id\}$ and hence $H' = \{id\}$ (G is Abelian). In this case $K' = K = \mathbb{Q}(\xi_p)$ and $R' = R = S^{-1}$.

Proposition 1 : (K,S) is a non simple CM type if and only if there exists a nontrivial subgroup G_1 of odd order such that $S = \bigcup_{t \in T} G_1 t$ for some subset $T \subset G$.

Proof :

($\Rightarrow$) Suppose S is non simple, then $H = H' \neq \{1\}$. Then H is a cyclic subgroup of G, generated by an element a, of order m>1.

For any $t \in G$, $t \in S$ or $(-t) \in S$ but not both. If $t \in S$ then $Ht \subset S$. In particular, if $1 \in S$ then $H \subset S$ and m is odd (since if m is even, $a^{m/2} = -1 \in S$) . On the other hand , if $-1 \in S$ then $-H \subset S$ and m is also odd (if m is even, $-a^{m/2} = -(-1) = 1 \in S$). Therefore we can choose $G_1 = H$ and T as a set of representatives in S for the cosets of

H which lie in S .

($\Leftarrow$) Suppose $S = G_1T$, then for any $g \in G_1$: $gS \subset S$. Therefore $H \neq \{id\}$ and S is non simple.

<u>Proposition 2</u> : For any $a \in G$:

i) If S is simple, so is aS .

ii) If (K,S) is simple , rank (K,S) = rank (K,aS).

<u>Proof</u> : Let $S_1 = S$, $S_2 = aS$ and H_1 and H_2 are the corresponding subgroups.

i) If aS is non simple then $g \in H_2$ for some $g \neq 1$. But then $g \in H_1$, i.e H_1 is non trivial, for $a \neq 1$. So S is non simple : contradiction.

ii) Note that $R'_1 = R_1 = a^{-1}R_2 = a^{-1}R'_2$, $K'_1 = K'_2 = \mathbb{Q}(\xi_p)$.

Consider $\phi_i : X(K) \to X(K'_i)$

$$[\sigma] \to \sum_{r' \in R'_i} [r'\sigma] \qquad i = 1,\ 2$$

For any $j \in G$: $\phi_1[j] = \sum_{r' \in R'_1} [r'j] = \phi_2[a^{-1}j]$ (note that G is cyclic hence Abelian).

Then $\mathrm{Im}\phi_1 = \mathrm{Im}\phi_2$, i.e rank (K,S) = rank (K,aS) .

<u>Proposition 3</u> : The number of non simple CM types in $K = \mathbb{Q}(\xi_p)$ is :

$$\sum_{d_i \in P_p} 2^{((p-1)/2d_i)} - \sum_{d_i \neq d_j;\, d_i, d_j \in P_p} 2^{((p-1)/2d_id_j)} + \dots$$

$$+ (-1)^{(t-1)} \cdot 2^{((p-1)/2 \prod_{d_i \in P_p} d_i)}$$

in which P_p is the set of all odd rational primes d_i such that $d_i \,\Big|\, \frac{p-1}{2}$

and $t = |P_p|$.

Proof : At first note that the number of CM types in K is $2^{(p-1)/2}$ (each CM type is a set of coset representatives of $\{1,-1\}$).
Let S be a non simple CM type, with the corresponding subgroup H $\neq \{1\}$. Let H be of order m . By proposition 1, m is an odd integer.
Given a subgroup H of odd order m , we can form $2^{(p-1)/2m}$ non simple CM types S with corresponding subgroup H (since if $g \in S$ then $gH \subset S$, else $-gH \subset S$) . Moreover, given $m \mid \frac{p-1}{2}$, m odd , we can find only 1 cyclic subgroup of G of order m . Therefore, by counting principle :

$$\begin{aligned}
&\#\text{ non simple CM types} \\
&= \sum_{\text{odd } m \mid (p-1)/2;\, m>1} 2^{((p-1)/2m)} \\
&= \sum_{d_i \in P_p} 2^{((p-1)/2d_i)} - \sum_{d_i \neq d_j;\, d_i, d_j \in P_p} 2^{((p-1)/2d_i d_j)} + \dots \\
&\qquad + (-1)^{(t-1)} 2^{((p-1)/2 \prod_{d_i \in P_p} d_i)}
\end{aligned}$$

Corollary 1 :

$$\#\text{ simple CM types} = 2^{((p-1)/2)} - \Big(\sum_{d_i \in P_p} 2^{((p-1)/2d_i)} - \sum_{d_i \neq d_j;\, d_i, d_j \in P_p} 2^{((p-1)/2d_i d_j)} + \dots + (-1)^{(t-1)} 2^{((p-1)/2 \prod_{d_i \in P_p} d_i)} \Big)$$

and the RHS is divisible by p-1.

Proof : The first assertion is obvious, while the second assertion follows from the fact that $\sim$ is an equivalence relation on the set of simple CM types in K and proposition 2(ii) ($S \sim S'$ iff $S = aS'$ for some $a \in G$)

2.2 Ranks of simple CM types in $\mathbb{Q}(\xi_p)$:

In this section we will study the rank of a CM type (K,S) in terms of characters.

Note that a character χ of an Abelian group G is a group homomorphism from G into $\mathbb{C}^*$. In the case $G = (\mathbb{Z}/p\mathbb{Z})^*$ is generated by an element r , χ is a homomorphism χ_h for some $0 \leq h < p-1$:

$$\chi_h : G \rightarrow U = \{ z \in \mathbb{C} \;/\; |z| = 1 \}$$
$$r^k \rightarrow \exp\left(\frac{2\pi i h k}{p-1}\right) \qquad \text{for all } k = 0,\dots, p-2$$

Theorem 1 (Kubota) : Let (K,S) be a simple CM type, in which $G = \mathrm{Gal}(K/\mathbb{Q})$ is Abelian. Then

$$\mathrm{rank}\ (K,S) = \#\{ \text{ character } \chi \in \mathrm{Hom}(G,\mathbb{C}^*) : \sum_{s \in S} \chi(s) \neq 0 \}$$

At first we need a lemma :

Lemma 1 : For each $\chi \in \mathrm{Hom}(G,\mathbb{C}^*)$ let $\nu_\chi = \frac{1}{|G|}\sum_{g \in G} \overline{\chi}(g)g$. Then $\{ \nu_\chi \;/\; \chi \in \mathrm{Hom}(G,\mathbb{C}^*) \}$ form a basis of $\mathbb{C}[G]$ (considered as a vector space over $\mathbb{C}$).

Proof of lemma 1 :

For $h \in G$:
$$\sum_{\chi \in \mathrm{Hom}(G,\mathbb{C}^*)} \chi(h)\nu_\chi = \sum_\chi \chi(h)\frac{1}{|G|}\sum_{g \in G}\overline{\chi}(g)g$$
$$= \frac{1}{|G|}\sum_{g \in G}\sum_\chi \chi(hg^{-1})g = h$$

$$\left(\text{since } \overline{\chi}(g) = \chi^{-1}(g) = \chi(g^{-1})\right.$$

$$\left.\text{and } \sum_{\chi\in \mathrm{Hom}(G,\mathbb{C}^*)} \chi(k) = \begin{cases} |G| & \text{if } k=1 \\ 0 & \text{if } k\neq 1 \end{cases}\right)$$

Moreover $\dim_{\mathbb{C}} \mathbb{C}[G] = \#\{\nu_\chi / \chi \in \mathrm{Hom}(G,\mathbb{C}^*)\} = |G| = p-1$

Therefore $\{\nu_\chi / \chi \in \mathrm{Hom}(G,\mathbb{C}^*)\}$ form a basis of $\mathbb{C}[G]$

Proof of theorem 1 :

Consider $\lambda : \mathbb{Z}[G] \to \mathbb{Z}[G]$

$$\sum_{g\in G} a_g g \to \sum_{g\in G} \left(\sum_{s\in S} a_g (gs)\right)$$

Extend λ into $\overline{\lambda} : \mathbb{C}[G] \to \mathbb{C}[G]$

$$\nu_\chi \to \frac{1}{|G|} \sum_{g\in G} \overline{\chi}(g)\lambda(g)$$

Note that rank $(K,S) = \mathrm{rank}_{\mathbb{Z}} \mathrm{Im}\lambda = \dim_{\mathbb{C}} \mathrm{Im}\overline{\lambda}$

We have :

$$\begin{aligned}
\overline{\lambda}(\nu_\chi) &= \frac{1}{|G|}\sum_{g\in G} \overline{\chi}(g)\lambda(g) \\
&= \frac{1}{|G|}\sum_{g\in G} \overline{\chi}(g)\left(\sum_{s\in S} gs\right) \\
&= \frac{1}{|G|}\sum_{s\in S}\sum_{g\in G} \overline{\chi}(g)gs \\
&= \frac{1}{|G|}\sum_{s\in S}\chi(s) \sum_{g\in G} \overline{\chi}(gs)gs \quad (\text{since } \overline{\chi}(g) = \overline{\chi}(gs)\chi(s)) \\
&= \sum_{s\in S}\chi(s)\frac{1}{|G|}\sum_{g\in G} \overline{\chi}(gs)gs \\
&= \sum_{s\in S}\chi(s).\nu_\chi
\end{aligned}$$

Therefore $\overline{\lambda}$ is diagonal with respect to this basis.

$$\dim_{\mathbb{C}} \mathrm{Im}\overline{\lambda} = \#\{\text{character } \chi : \sum_{s\in S} \chi(s) \neq 0\}$$

Corollary 2 : If (K,S) is simple, rank (K,S) = 1 + #{odd character χ : $\sum_{s\in S}\chi(s) \neq 0$ }

Proof :

If χ = id then $\sum_{s\in S}\chi(s) = \frac{|G|}{2} \neq 0$

If $\chi \neq$ id and χ is even :

$$\chi(-g) = \chi(g) \quad \Rightarrow \quad \sum_{s\in S}\chi(s) = \sum_{s\notin S}\chi(s) = 0$$

Note that to prove theorem 1, we need only that G is Abelian.

In the case K = $\mathbb{Q}(\xi_p)$, G = Gal(K/$\mathbb{Q}$) is a cyclic group generated by r, then a CM type S can be expressed as :

$$S = \sum_{k=0}^{((p-1)/2\ -\ 1)} \eta_k r^k$$

in which $\eta_k = 1$ or $\eta_k = r^{(p-1)/2}$

Let $I_S \doteq \{ k \ / \ \eta_k = r^{(p-1)/2} \} \subset \{ 0, 1, ..., (p-1)/2 - 1 \}$

Then we can associate with a CM type S a subset I_S of { 0, 1 ,..., (p-1)/2 - 1 }

Proposition 4 : Let (K,S) be a CM type, K = $\mathbb{Q}(\xi_p)$. Then

$$\text{Rank } (K,S) = \frac{p+1}{2} - \#\{ h \text{ odd} : 1 \leq h < p\text{-}1 \text{ and}$$
$$\sum_{k\in I_S} \cos\left(\frac{2\pi hk}{p-1}\right) = \frac{1}{2} \quad \text{and} \quad \sum_{k\in I_S} \sin\left(\frac{2\pi hk}{p-1}\right) = \frac{1}{2} \cdot \frac{\sin(2\pi h/(p-1))}{1-\cos(2\pi h/(p-1))} \}.$$

Proof :

A character χ of G = $(\mathbb{Z}/p\mathbb{Z})^*$ = <r> has the form χ_h for some $0 \leq h < p-1$: $\chi_h(r^k) = \exp(\frac{2\pi i hk}{p-1})$, k=0,1,...,p-2 and χ_h is odd iff h is odd.

Now we consider a character χ_h , h is odd such that $\sum_{s\in S}\chi_h(s) = 0$

We have :

$$\sum_{s\in S}\chi_h(s) = \sum_{k=0}^{((p-1)/2\ -\ 1)} \chi_h(r^k) - 2\sum_{k\in I_S}\chi_h(r^k)$$

A direct calculation gives us :

$$\sum_{k=0}^{((p-1)/2\ -\ 1)} \chi_h(r^k) = \sum_{k=0}^{((p-1)/2\ -\ 1)} \exp(\frac{2\pi ihk}{p-1})$$

$$= 1 + \frac{\sin(2\pi h/(p-1))}{1-\cos(2\pi h/(p-1))} \ .\ i$$

We have :

$$\sum_{k\in I_s}\chi_h(r^k) = \sum_{k\in I_S}\cos(\frac{2\pi hk}{p-1}) + (\sum_{k\in I_s}\sin(\frac{2\pi hk}{p-1}))\ .\ i$$

Then $\sum_{s\in S}\chi_h(s) = 0$ if and only if

$$\sum_{k\in I_s}\cos(\frac{2\pi hk}{p-1}) = \frac{1}{2}$$

and $$\sum_{k\in I_s}\sin(\frac{2\pi hk}{p-1}) = \frac{1}{2}\ .\ \frac{\sin(2\pi h/(p-1))}{1-\cos(2\pi h/(p-1))}$$

The conclusion follows from the fact that :

$$1 + \#\{\text{ odd character } \chi\ \} = \frac{p+1}{2}$$

<u>Corollary 3</u> : If $card(I_S) = 1$ and $6 \nmid (p-1)$ or $12|(p-1)$ then S is nondegenerate.

<u>Proof</u> :

Suppose $I_S = \{t\}$ and there exists an odd integer $h < (p-1)$ such that

(*) $$\cos(\frac{2\pi ht}{p-1}) = \frac{1}{2} \quad \text{and} \quad \sin(\frac{2\pi ht}{p-1}) = \frac{1}{2}\ .\ \frac{\sin(2\pi h/(p-1))}{1-\cos(2\pi h/(p-1))}$$

Then $\left| \frac{1}{2} \cdot \frac{\sin(2\pi h/(p-1))}{1-\cos(2\pi h/(p-1))} \right| = \frac{\sqrt{3}}{2}$

$$\Rightarrow 4\cos^2\left(\frac{2\pi h}{p-1}\right) - 6\cos\left(\frac{2\pi h}{p-1}\right) + 2 = 0$$

$$\Rightarrow \cos\left(\frac{2\pi h}{p-1}\right) = 1 \text{ or } \frac{1}{2}$$

If $\cos\left(\frac{2\pi h}{p-1}\right) = 1$ then $h = 0$: contradiction since h is odd.

If $\cos\left(\frac{2\pi h}{p-1}\right) = \frac{1}{2}$ then $h = \frac{p-1}{6} \notin N$ or $h = \frac{p-1}{6}$ is an odd integer, contradicting our hypothesis on p .

Therefore S is nondegenerate, i.e rank $(K,S) = \frac{p+1}{2}$.

<u>Corollary 4</u> : If $\mathrm{card}(I_S) = 1$ then rank $(K,S) \geq \frac{p-1}{2}$.

<u>Proof</u> : If $\mathrm{card}(I_S) = 1$ then $h = \frac{p-1}{6}$. Therefore $\#\{ \chi \text{ odd} : \sum_{s\in S} \chi(s) = 0 \} \leq 1$

<u>Corollary 5</u> : Let (K,S) be a simple CM type, $K = \mathbb{Q}(\xi_p)$ in which $p \equiv 1 (\bmod 4)$. Then

$$\text{rank } (K,S) \geq 1 + \frac{1}{2} \cdot \frac{p-1}{2} \quad \text{if } p \equiv 1 \ (\bmod 8)$$

$$\geq \frac{1}{2} \cdot \frac{p-1}{2} \quad \text{if } p \equiv 5 \ (\bmod 8)$$

<u>Proof</u> :

Consider $S = \sum_{k=0}^{((p-1/2 - 1)} \eta_k r^k$, $\eta_k = 1$ or $\eta_k = r^{(p-1)/2}$. Then we can write $S = \sum_{k'\in J} r^{k'}$, in which J is a subset of $\{ 0, 1,\ldots,p-2 \}$. If J doesn't contain 2 consecutive integers then S is not a CM type (if $J = \{ 1, 3, 5,\ldots,p-2 \}$ then S contains $\{ r^1, -r^1 = r^{(p-1)/2}.r^1 = r^{(p+1)/2} \}$, on the other hand if $J = \{ 0, 2, 4,\ldots, p-3 \}$ then S contains $\{ r^2, -r^2 \}$). Therefore given a simple CM type S, we can find $a \in G$ such that for $S_1 = aS$ we have $\{ r^{(p-3)/2}, r^{(p-1)/2} \} \subset S$, i.e $0 \in I_{S_1}$, $\frac{p-3}{2} \notin I_{S_1}$. Note that rank (K,S) = rank (K,S_1). Since $p \equiv 1 (\text{mod } 4)$, then if h is odd, so is $(p-1)/2 - h$.

Suppose that $p \equiv 1$ (mod 8) and rank $(K,S) < 1 + \frac{1}{2} \cdot \frac{p-1}{2}$, then $\#\{ h \text{ odd} : \sum_{s \in S} \chi_h(s) = 0 \} > \frac{1}{2} \cdot \frac{p-1}{2}$. Since we can partition the set of odd integers from 0 to p-2 into $(p-1)/4$ subsets of the form $\{ h, (p-1)/2 - h \}$, each containing 2 elements, then by the pigeon hole principle, there exists an h odd such that $\sum_{s \in S_1} \chi(s) = \sum_{s \in S_1} \chi_{(p-1)/2 - h}(s) = 0$. Then

$$\sum_{k \in I_{S_1}} \cos\left(\frac{2\pi hk}{p-1}\right) = \sum_{k \in I_{S_1}} \cos\left(\frac{2\pi((p-1)/2 - h)k}{p-1}\right) = \frac{1}{2}$$

For the CM type S_1 :

$$\sum_{k \text{ odd} \in I_{S_1}} \cos\left(\frac{2\pi hk}{p-1}\right) + \sum_{k \text{ even} \in I_{S_1}} \cos\left(\frac{2\pi hk}{p-1}\right) = \frac{1}{2}$$

$$-\sum_{k \text{ odd} \in I_{S_1}} \cos\left(\frac{2\pi hk}{p-1}\right) + \sum_{k \text{ even} \in I_{S_1}} \cos\left(\frac{2\pi hk}{p-1}\right) = \frac{1}{2}.$$

Then :
$$\sum_{k \text{ odd} \in I_{S_1}} \cos\left(\frac{2\pi hk}{p-1}\right) = 0 \qquad (*)$$

$$\sum_{k \text{ even} \in I_{S_1}} \cos\left(\frac{2\pi hk}{p-1}\right) = \frac{1}{2}$$

Let $S_2 = r^1 S_1$ then $\{0\} \subset I_{S_2}$. Note that if h is odd such that

$\sum_{s\in S_1} \chi_h(s) = 0$ then $\chi_h(r) \sum_{s\in S_1} \bar{\chi}_h(s) = 0$, i.e $\sum_{s\in S_2} \chi_h(s) = 0$. Moreover $\{ k \in I_{S_2}, k \text{ odd} \} = \{ k \in I_{S_1}, k \text{ even} \}$ and $\{ k \in I_{S_2}, k \text{ even} \} = \{ k \in I_{S_1}, k \text{ odd} \} \cup \{0\}$. From (*), we have :

$$\sum_{k \text{ odd } \in I_{S_2}} \cos(\frac{2\pi hk}{p-1}) = \frac{1}{2} \quad \text{and} \quad \sum_{k \text{ even } \in I_{S_2}} \cos(\frac{2\pi hk}{p-1}) = 1 \qquad (**)$$

But if we apply the same argument for S_2, we have :

$$\sum_{k \text{ odd } \in I_{S_2}} \cos(\frac{2\pi hk}{p-1}) = 0 \text{ and } \sum_{k \text{ even } \in I_{S_2}} \cos(\frac{2\pi hk}{p-1}) = \frac{1}{2}$$

This contradicts with (**)

Therefore :

$$\text{rank } (K,S) \geq 1 + \frac{1}{2}.\frac{p-1}{2}$$

Now suppose $p \equiv 5 \pmod 8$ then if $\text{rank}(K,S) < \frac{1}{2} . \frac{p-1}{2}$ then $\#\{ h \text{ odd} : \sum_{s\in S} \chi_h(s) = 0 \} > 1 + \frac{1}{2} . \frac{p-1}{2}$. Since we can partition the set of odd integers from 0 to p-2 into $(p-1)/4 + 1$ subsets of the form $\{ h , (p-1)/2 - h \}$, each containing 2 elements except two subsets containing 1 element, then by the similar argument we get a contradiction. Therefore in this case we have :

$$\text{rank } (K,S) \geq \frac{1}{2}.\frac{p-1}{2}$$

Chapter 3

CM types of Fermat curves

3.1 Fermat curves and the corresponding CM types

Denote by $F(N)$ the Fermat curves :

$$X^N + Y^N + Z^N = 0$$

In [3], Fadeev has proved that the Jacobian of the Fermat curve $F(p)$, p being an odd prime can be factored as:

$$\mathrm{Jac}(F(p)) \simeq \prod_{a=1}^{p-2} \mathrm{Jac}(F_{1,a})$$

in which $F_{1,a}$ is the curve whose basis for the holomorphic 1-forms is $\{ \omega_{\langle g\rangle,\langle ga\rangle} : 1 \le g \le p,\ 1 \le \langle g\rangle, \langle ga\rangle, \langle g\rangle+\langle ga\rangle < p \}$ ($\langle k\rangle$ is the unique integer satisfying $0 \le \langle k\rangle < p$, $\langle k\rangle \equiv k$ (mod p) and $\omega_{r,s} = x^{r-1}y^{s-1}d(x)/y^{p-1}$ for $x = X/Z$, $y = Y/Z$ and $Z \neq 0$)

Let $S_a = \{ g \in G = \mathrm{Gal}(\mathbb{Q}(\xi_p)/\mathbb{Q}) : \langle g\rangle + \langle ag\rangle < p \}$ It is easy to check that (K,S_a) is a CM type ($K = \mathbb{Q}(\xi_p)$), which is called the CM type corresponding to the factor curve $F_{1,a}$.

Proposition 1 : Let (K,S_a) be a CM type, $1 \le a \le p-2$. Then :

i) $S_{p-1-a} = S_a$

ii) S_a and $S_{a^{-1}}$ have the same rank.

Proof :

$$\begin{aligned} \text{i) } S_{p-1-a} &= \{ g\in G : \langle g\rangle + \langle (p-1-a)g\rangle < p \} \\ &= \{ g\in G : \langle g\rangle + \langle -(a+1)g\rangle < p \} \\ &= \{ g\in G : \langle g\rangle + p - \langle (a+1)g\rangle < p \} \end{aligned}$$

For some $g \in S_a$, suppose $<g> > <(a+1)g>$. Then $<g> > <ag+g> = <ag> + <g>$ (since $g \in S_a$). But this leads to a contradiction since $<ag> \geq 1$.

Therefore if $g \in S_a$, $<g> + p - <(a+1)g> < p$, i.e $g \in S_{p-1-a}$. In other words, $S_a \subset S_{p-1-a}$.

Since S_a, S_{p-1-a} are CM types, we have : $S_a = S_{p-1-a}$

ii) We have $S_{a^{-1}} = \{ g' : <a^{-1}g'> + <g'> < p \}$

$$= \{ ag : <g> + <ag> < p \}$$

$$= aS_a$$

By proposition 2, chapter 2 : rank (K,S_a) = rank $(K,S_{a^{-1}})$

3.2 Ranks of CM types of Fermat curves :

For the CM type (K,S_a), $K=\mathbb{Q}(\zeta_p)$, $1 \leq a \leq p-2$, an alternative expression can be obtained for the rank.

Theorem 1 (Kubota) :

$$\text{rank } (K,S_a) = 1 + \#\{ \text{ odd character } \chi : \chi(a+1) \neq \chi(a) + 1 \}$$

Proof :

Consider an odd character χ of Gal(K/Q). It is known that $\frac{1}{p}\sum_{b=1}^{p-1} \chi(b)b \neq 0$ since the left hand side is the value at $s=0$ of the Dirichlet L-function $L(s,\chi)$ and $L(s,\chi)$ does not vanish on the line $Re(s) = 0$.

We have :

$$L(0,\chi).(1 + \bar{\chi}(a) - \bar{\chi}(a+1))$$
$$= \frac{1}{p} \Big(\sum_b \chi(b)b + \sum_b \chi(b)\bar{\chi}(a)b - \sum_b \chi(b)\bar{\chi}(1+a)b \Big)$$
$$= \frac{1}{p} \Big(\sum_c \chi(c)c + \sum_c \chi(c)<ac> - \sum_c \chi(c)<(1+a)c> \Big)$$

$$= \frac{1}{p}\left(\sum_{c=1}^{p-1} (<c> + <ac> - <(1+a)c>) \right) \chi(c)$$

Since $<c> + <ac> - <(1+a)c> = 0$ if $c \in S_a$

$= p$ if $c \notin S_a$.

Then $L(0,\chi).(1 + \bar{\chi}(a) - \bar{\chi}(a+1)) = \sum_{s \notin S_a} \chi(s) = - \sum_{S \in S_a} \chi(s)$

But $L(0,\chi) \neq 0$, then $\sum_{s \in S} \chi(s) = 0$ if and only if $\bar{\chi}(a+1) = \bar{\chi}(a) + 1$,

i.e $\chi(a+1) = \chi(a) + 1$

This concludes the proof.

The condition $\chi(a+1) = \chi(a) + 1$ is equivalent to having $\chi(a) = \exp(+\frac{2\pi i}{3})$, $\chi(a+1) = \exp(+\frac{2\pi i}{6})$ or $\chi(a) = \exp(-\frac{2\pi i}{3})$, $\chi(a+1) = \exp(-\frac{2\pi i}{6})$. Therefore we have :

<u>Proposition 2</u> : If $(p-1,3) = 1$ then S_a is nondegenerate for all a , $1 \leq a \leq p-2$.

<u>Proof</u> : Obvious, since $(p-1,3) = 1$ implies $\chi(g) \neq \exp(\pm \frac{2\pi i}{6})$ for all $g \in G$.

<u>Proposition 3</u> : For $1 \leq a \leq p-2$:

i) If $(\mathrm{ord}(a),3) = 1$ then S_a is nondegenerate.

ii) If $\mathrm{ord}(a) = 6t$, $t \in \mathbb{N}$ then S_a is nondegenerate.

iii) If $\mathrm{ord}(a) = 3$ then S_a is non simple.

<u>Proof</u> :

i) If $\chi(a) = \exp(\pm\frac{2\pi i}{3})$ and $(\mathrm{ord}(a),3) = 1$ then

$$\chi(a^{\mathrm{ord}(a)}) = (\chi(a))^{\mathrm{ord}(a)} = (\exp(\pm\frac{2\pi i}{3}))^{\mathrm{ord}(a)} \neq 1$$

But $\chi(a^{\mathrm{ord}(a)}) = \chi(1) = 1$

Therefore rank $S_a = 1 + \#\{\text{ odd character } \chi\} = 1 + \frac{p-1}{2}$

ii) Suppose $\chi(a) = \exp(\pm\frac{2\pi i}{3})$ and $\mathrm{ord}(a) = 6t$

$$\chi(a^{3t}) = (\chi(a)^3)^t = (\exp(\pm\frac{2\pi i}{3}))^{3t} = 1^t = 1$$

But if χ is odd :

$$\chi(a^{3t}) = \chi(-1) = -1$$

Then S_a is nondegenerate.

iii) If $\mathrm{ord}(a) = 3$ then $1+a+a^2 = 0$

We have

$$\begin{aligned} aS_a &= \{ ag : \langle g\rangle + \langle ag\rangle < p \} \\ &= \{ g' : \langle a^{-1}g'\rangle + \langle g'\rangle < p \} \\ &= \{ g' : \langle a^2g'\rangle + \langle g'\rangle < p \} \\ &= S_{a^2} = S_{p-1-a} = S_a \text{ (by proposition 1)} \end{aligned}$$

Therefore S_a is non simple.

Indeed the converse of iii) is also true. See [7]

Now we want to obtain a lower bound for the ranks of all CM types S_a, $1 \le a \le p-2$, in which $(p-1,3) \neq 1$, i.e $6|(p-1)$. By proposition 3, we need only to consider the case $\mathrm{ord}(a) = 3q$, in which q is an odd integer greater than 1. At first, we need 2 lemmas :

<u>Lemma 1</u> : Let p be a prime such that $9|(p-1)$, and $G_1 = \langle b\rangle$ be the cyclic subgroup of order 9 in $G = (\mathbb{Z}/p\mathbb{Z})^*$. If b^i, b^j be 2 different generators of G_1 then $1+b^i+b^j \neq 0$ (in G).

<u>Proof</u>

Without loss of generality, we may assume that i=1. Suppose

$1+b+b^j = 0$, in which $j = 2, 4, 5, 7$ or 8. Note that $1+b^3+b^6 = 0$ and G_1 doesn't contain the subgroup $\{1,-1\}$ of order 2 of G.

If $j = 2$ then $1+b+b^2 = 0$ and then $-b-b^2-b^3 = 0$, hence $b^3 = 1$: contradiction.

If $j = 4$ then $1+b+b^4 = 0$ and then $-b-b^4-b^7 = 0$, hence $b^7 = 1$: contradiction.

If $j = 5$ then $1+b+b^5 = 0$ and then $-b^4-b^5-1 = 0$, hence $b = b^4$, i.e $b^3 = 1$: contradiction.

If $j = 7$ then $1+b+b^7 = 0$ and since $-b-b^4-b^7 = 0$, hence $b^4 = 1$: contradiction.

If $j = 8$ then $1+b+b^8 = 0$ and so $1+b+b^2 = 0$: again contradiction.

This concludes the prooof.

<u>Lemma 2</u>: Let p be a prime such that $15 | (p-1)$ and $G_2 = <c>$ be the subgroup of order 15 in $G = (\mathbb{Z}/p\mathbb{Z})^*$. If $i = 1, 4, 7$ or 13 and $i' = 2, 8, 11$ or 14 then $1+c^i+c^{i'} \neq 0$ (in G)

<u>Proof</u> :

Similarly, we may assume that $i = 1$. Suppose that $1+c+c^{i'}$, in which $i' = 2, 8, 11, 14$. Note that we have $1+c^5+c^{10} = 0$

If $1+c+c^2 = 0$ then $c+c^2+c^3 = 0$ and so $c^3 = 1$: contradiction.

If $1+c+c^8 = 0$ then $c^7+c^8+1 = 0$ and so $c^6 = 1$: contradiction.

If $1+c+c^{11} = 0$ then, combining with $c+c^6+c^{11} = 0$ we have $c^6 = 1$: contradiction.

If $1+c+c^{14} = 0$ then $c+c^2+1 = 0$ and $c^{12} = 1$: again contradiction.

This concludes the proof.

<u>Theorem 2</u> : Let (K,S_a) be a simple CM type, $1 \leq a \leq p-2$ and $K = Q(\xi_p)$, $6 \nmid (p-1)$. Then :

$$\text{rank } (K,S_a) \geq 1 + \frac{1}{2} \cdot \frac{19}{21}(p-1)$$

<u>Proof</u> :

Denote $w = \exp(\frac{2\pi i}{6})$

Now we want to find all odd characters χ such that $\chi(a+1) = \chi(a) + 1$.

Let $p-1 = 2^k.3^t.m$, in which $(m,6) = 1$, and let r be a primitive root mod p . Write $a = r^{2^{k'}.3^{t'}.m'}$ in which $(m',6) = 1$.

Then we have :

$$\text{ord}(a) = (p-1)/\gcd(p-1,2^{k'}.3^{t'}.m')$$

By proposition 3, we have :

. If $t' \geq t$: S_a is nondegenerate.

. Suppose $t' < t$. If $k' < k$ then $6 | \text{ord}(a)$ and then S_a is nondegenerate.

Therefore without loss of generality, we may assume that $a = r^{2^{k'}.3^{t'}.m'}$ in which $k' \geq k$, $t'<t$ and $(m',6) = 1$. Note that for such odd character χ, $\chi(a) = w^{\pm 2}$, $\chi(-1) = \chi(r^{2^{k-1}.3^t.m}) = -1$

<u>case 1</u> : $\chi(a) = w^2$

In this case :

$$\chi(r^{\gcd(2^{k'}.3^{t'}.m' \,,\, 2^{k-1}.3^t.m)})$$

$$= \chi(r^{2^{k'}.3^{t'}.m'.q' + 2^{k-1}.3^t.m.q})$$

$$= \chi(r^{2^{k'}.3^{t'}.m'})^{q'} \;.\; \chi(r^{2^{k-1}.3^{t}.m})^{q}\,.$$
$$= (w^2)^{q'}.(-1)^q \qquad \text{for some } q,q'\in\mathbf{Z}$$

Since $k' \geq k$, $t' < t$, $q \not\equiv 0 \pmod 2$ and $q' \not\equiv 0 \pmod 3$. Therefore $\chi(r^{2^{k-1}.3^{t'}.\gcd(m,m')}) = w^{\pm 1}$ and exactly one of these occurs.

If $2^{k-1}.3^{t'}.\gcd(m,m') = 2^{k-1}.3^{t-1}.m$ then $\mathrm{ord}(a) = 3$, hence S_a is non simple, by proposition 3. Therefore we may assume that $2^{k-1}.3^{t'}.\gcd(m,m')$ is a proper divisor of $2^{k-1}.3^{t-1}.m$

Since for any fixed $g\in U$, $\#\{\text{character } \chi : \chi(r^b) = g\} = b$, then

$$\#\{\text{ odd character } \chi : \chi(a+1) = \chi(a) + 1, \chi(a) = w^2 \}$$
$$\leq 2^{k-1}.3^{t'}.\gcd(m,m')$$
$$= \frac{1}{2.3.n}(2^k.3^t.m) = \frac{1}{2.3.n}(p-1)$$

in which n is an odd integer.

<u>if $n = 3$</u> : then $\gcd(2^{k'}.3^{t'}.m' , 2^{k-1}.3^{t}.m) = 2^{k-1}.3^{t-2}.m$

This implies $t' = t-2$, $m \mid m'$

$$a = r^{2^k.3^{t-2}.m.i} \text{ for some } 1\leq i\leq 8 \text{ , } i \neq 3,6$$

Since $S_a = S_{p-1-a}$ by proposition 1, we can apply the same argument for S_{p-1-a} , and then

$$p-1-a = r^{2^k.3^{t-2}.m.i'} \text{ for some } 1\leq i'\leq 8 \text{ , } i' \neq 3,6$$

By lemma 1; this happens if and only if $p-1-a \equiv a$. In other words, $a+1 \equiv -a$

But then $\chi(a+1) = \chi(-a) = -\chi(a) \qquad (\chi \text{ is odd})$

$$\chi(a) + 1 = -\chi(a)$$
$$\chi(a) = -\frac{1}{2} \text{ : a contradiction.}$$

<u>if $n = 5$</u> : then $p-1 = 2^k.3^t.5^u.m$ in which $(m,30) = 1$

Let $a = r^{2^k.3^{t-1}.5^{u-1}.m.i}$ and $a+1 = r^{2^{k-1}.3^{t-1}.5^{u-1}.m.j}$, with $i \leq 15$ and $j \leq 30$:

If $\chi(r^{2^{k-1}.3^{t-1}.5^{u-1}.m}) = w$, $\chi(a) = w^2$ implies $2i \equiv 2 \pmod 6$, i.e $i = 1, 4, 7, 13$ ($i \neq 10$ since otherwise ord(a) $= 3$ and S_a is then non simple). Moreover, $\chi(a+1) = w$ and so $j \equiv 1 \pmod 6$, i.e $j = 1, 7, 13, 19, 25$

Then $p-1-a \equiv -(a+1) \pmod p$

$$= r^{(2^{k-1}.3^t.5^u.m)} \cdot r^{(2^{k-1}.3^{t-1}.5^{u-1}.m.j)}$$

$$= r^{(2^{k-1}.3^{t-1}.5^{u-1}.m(j+15))}$$

in which $j+15 = 2.8, 2.11, 2.14, 2.2$ or 2.5 . Since $S_a = S_{p-1-a}$ then $j+15 \neq 2.5$ (otherwise, p-1-a has order 3 and this would imply $S_a = S_{p-1-a}$ is non simple).

Now $p-1-a = r^{(2^k.3^{t-1}.5^{u-1}.m.i')}$ for some $i' = 2, 8, 11, 14$. Since we have $1 + (a) + (p-1-a) \equiv 0 \pmod p$ then again this contradicts our lemma 2.

If $\chi(r^{2^{k-1}.3^{t-1}.5^{u-1}.m}) = w^{-1}$, $\chi(a) = w^2$ implies $i = 2, 8, 11, 14$ and $\chi(a+1) = w$ implies $j = 5, 11, 17, 23, 29$ and $j+15 = 2.10, 2.13, 2.1, 2.4$ or 2.7 , $j+15 \neq 2.10$

Again, this contradicts our lemma 2.

Therefore

$$\#\{ \text{ odd character } \chi : \chi(a+1) = \chi(a) + 1, \chi(a) = w^2 \}$$
$$\leq \frac{1}{2.3.7}(p-1)$$

<u>case 2</u> : $\chi(a) = w^{-2}$

By the similar argument, we have :

$$\#\{ \text{ odd character } \chi : \chi(a+1) = \chi(a) + 1,\ \chi(a) = w^{-2} \} \leq \frac{1}{2.3.7}(p-1).$$

Therefore rank $S_a \geq \frac{p+1}{2} - 2.\frac{1}{2.3.7}(p-1)$

$$= 1 + \frac{19}{42}(p-1)$$

Example 1 : A computer program was written and run by means of the VAX-750 system for all rational primes $p \leq 2000$. The worst case happens when $p = 271$, with $a = 32, 114, 126, 144, 156, 238$. Then

$$\text{rank } S_a = 126 = \frac{p+1}{2} - 10$$
$$= 1 + \frac{25}{54}(p-1)$$

For example, with $a = 32$ then $a = 6^{230}$ and $a+1 = 6^{85}$, we have

$$\mathrm{mod}(\frac{230}{5},6) \equiv 4 \equiv -2$$
$$\mathrm{mod}(\frac{85}{5},6) \equiv 5 \equiv -1$$

Then

$$\{ \chi \text{ odd } : \chi(a+1) = \chi(a) + 1 \}$$
$$= \{ \chi : \chi(6^5) = z \text{ or } \chi(6^5) = z^{-1} \}$$

Example 2 : The first rational prime p such that there exists a degenerate CM type S_a is $p = 67$, with $a = 6, 10, 19, 47, 56, 60$

$$\text{rank } S_a \neq 32 = \frac{p+1}{2} - 2$$

For example, with $a = 6$, $a = 2^{40}$, $a+1 = 2^{23}$, we have :

$$\mathrm{mod}\left(\frac{40}{1},6\right) = 4 = -2$$

$$\mathrm{mod}\left(\frac{23}{1},6\right) = 5 = -1$$

Then

$$\{\ \chi \text{ odd} : \chi(a+1) = \chi(a) + 1\ \}$$

$$= \{\ \chi : \chi(2) = z \text{ or } \chi(2) = z^{-1}\ \}$$

Chapter 4

The design and analysis of algorithms

In this chapter, we will design some algorithms, together with their analysis, to study the rank of CM types.

4.1 Algorithm 1 (* This algorithm is used to find the rank of a simple CM type (K,S) with a given Galois group G = Gal (K/Q) = { $1=g_1, g_2, \ldots, g_n$ } . A[i,j] is initialized as an (n,n)-matrix *)

Step 1 : i ← 2

Step 2 : j ← 0

Step 3 : Do j ← j+1 until (j>n) or (g[j]∈S and g[i]g[j]∉S)

Step 4 : If j>n then go to step 9 (* S is non simple , H ⊃ { id,g[i] } *)

else i ← i+1

Step 5 : If i ≤ n go to step 2

Step 6 : R = ϕ

For i=1 to n do

If $g[i]^{-1}$ ∈ S then R ← R ∪ { g[i] }

Step 7 : For i=1 to n do

For j=1 to n do

If g[j] ∈ R and g[i]g[j] = g[k] then A[i,k] ← 1

Step 8 : rank (K,S) ← rank A.

Step 9 : stop.

The maximal cost of algorithm 1 is $(3n^2-n-2) + (n^2+2n) = (4n^2+n-2)$ comparisons and $2n^2 + \sigma(n)$ multiplications, in which $\sigma(n)$

is the maximum number of multiplications needed to do step 8 (additions are omitted). By using the Gram-Schmidt procedure, we can show that $\sigma(n) \leq \frac{n^3}{3} - \frac{n}{3}$. Therefore in the worst case, algorithm 1 uses $O(n^2)$ comparisons and $O(n^3)$ multiplications.

4.2 Algorithm 2 (* This algorithm is used to find the rank of a CM type (K,S) with $K = Q(\xi_p)$, $G = Gal(K/Q) = \{ 1=g_1, g_2, \ldots, g_n \}$ a cyclic group generated by g_2 *).

Step 1 : $D \leftarrow 0$

$N \leftarrow 1$

Step 2 : $Sum \leftarrow 0$

For $J=1$ to $p-1$ do

If $mod(g_2^J, p) \in S$ then

$Sum \leftarrow Sum + \exp(\frac{2\pi iJN}{p-1})$

Step 3 : If $Sum = 0$ then $D \leftarrow D + 1$

Step 4 : $N \leftarrow N + 2$

If $N \leq p-1$ then go to step 2, else go to step 5.

Step 5 : rank $(K,S) \leftarrow \frac{p+1}{2} - D$

Step 6 : stop

The maximal cost of algorithm 2 is $\frac{p^2-1}{2}$ comparisons, $\frac{3(p^2-1)}{2}.p$ multiplications (additions are omitted) and $(p-1)^2$ exponential operators. Then in the worst case, algorithm 2 uses $O(p^2)$ comparisons, $O(p^2)$ multiplications and $O(p^2)$ exponential operators. Remark that this algorithm can be modified to be applied for the case that $G = Gal(K/Q)$ is not cyclic, but Abelian. Any Abelian group can be factored as a direct product of cyclic groups.

4.3 Algorithm 3 (* This algorithm is used to find the rank of a simple CM type (K,S_a), $1 \leq a \leq p-2$, $K = Gal(K/Q) = \{ g_1 = 1, g_2, \ldots, g_n \}$ a cyclic group generated by g_2 *)

Step 1 : $D \leftarrow 0$

$I, I' \leftarrow 0$

$J \leftarrow 1$

Step 2 : Do $I \leftarrow I+1$ until $\mathrm{mod}(g_2^{\,I} - a, p) = 0$

Do $I' \leftarrow I'+1$ until $\mathrm{mod}(g_2^{\,I'} - a - 1, p) = 0$

Step 3 : If $\exp(\frac{2\pi iIJ}{p-1}) + 1 = \exp(\frac{2\pi iI'J}{p-1})$ then $D \leftarrow D+1$

Step 4 : $J \leftarrow J+2$

if $J \leq p-1$ then go to step 3 else go to step 5.

Step 5 : rank $(K,S_a) \leftarrow \frac{p+1}{2} - D$

Step 6 : stop

The maximal cost of algorithm 3 is 3(p-1) comparisons and 5p multiplications and 3(p-1) exponential operators, i.e O(p) comparisons, O(p) multiplications and O(p) exponential operators.

4.4 Algorithm 4 (* This algorithm is used to find a lower bound for the ranks of simple CM types (K,S_a), $K = Q(\xi_p)$, $G = Gal(K/Q) = \{ 1, g_2, \ldots, g_n \}$ generated by g_2, $1 \leq a \leq p-2$ *)

Step 1 : Minrank $\leftarrow \frac{p+1}{2}$

Step 2 : If $\mathrm{mod}(p,6) \neq 0$ then go to step 4.

(* All the CM types are nondegenerate *)

Step 3 : For a=1 to p-2 do

If $a \neq (p-1)/3$ and $a \neq 2(p-1)/3$ then

Find rank S_a (* using algorithm 3 *)

If Minrank > rank S_a then Minrank $\leftarrow$ rank S_a

Step 4 : stop

The maximal cost of algorithm 4 is 1 + 3p(p-4) comparisons, 3 + 5p(p-4) multiplications and 3(p-1)(p-4) exponential operators. Then in the worst case, algorithm 4 uses $O(p^2)$ comparisons, $O(p^2)$ multiplications and $O(p^2)$ exponential operators.

<u>4.5 Algorithm 5</u> (* This algorithm is used to test whether the lower bound of the ranks of CM types (K,S_a), $K = \mathbb{Q}(\xi_p)$ in theorem 2, chapter 3 can be obtained for $N_1 \leq p \leq N_2$, provided a list of rational primes $\{p_1,\dots,p_k\}$ from N_1 to N_2 together with the corresponding primitive roots $\{r_1,\dots,r_k\}$ is given. Then for each p_i, $G_i = \mathrm{Gal}(\mathbb{Q}(\xi_{p_i})/\mathbb{Q}) = \{1=r_i^0, r_i^1, \dots, (r_i)^{p_i-2}\}$. Note that by example 1, chapter 4 , this lower bound is not obtained if $N_2 \leq 2000$ *)

(* Found is a Boolean variable, true if we can find a prime p such that the lower bound $1 + \frac{19}{42}(p-1)$ is obtained *).

Step 1 : Found $\leftarrow$ false

I $\leftarrow$ 1

Step 2 : If mod (p[I]-1,42) $\neq$ 0 then go to step 9

Step 3 : J $\leftarrow$ 1

Step 4 : If J > 42 then go to step 4

else J' $\leftarrow$ 0

Do J' $\leftarrow$ J'+1 until $\mathrm{mod}(r[I]^{J'} - (r[I]^{J.(p[I]-1)/42} - 1), p[I]) = 0$

Step 5 : If $\mathrm{mod}(J', \frac{p[I]-1}{42}) = 0$ and $\mathrm{mod}(J'/\frac{p[I]-1}{42}, 6) = 2$

then Found = true , go to step 10

else J $\leftarrow$ J+6, go to step 4

Step 6 : $J \leftarrow 5$

Step 7 : If $J > 42$ then go to step 9

else $J' \leftarrow 0$

Do $J' \leftarrow J'+1$ until mod($r[I]^{J'}$ - $(r[I]^{J.(p[I]-1)/42}$ - 1) , p[I]) = 0

Step 8 : If $\mathrm{mod}(J', \frac{p[I]-1}{42}) = 0$ and $\mathrm{mod}(J'/\frac{p[I]-1}{42}, 6) = 4$

then Found $\leftarrow$ true, go to step 10

else $J \leftarrow J+6$, go to step 7

Step 9 : $I \leftarrow I+1$

If $I \leq k$ go to step 2

else go to step 10.

Step 10 : stop

The maximal cost of algorithm 5 is $k(16+14N_2)$ comparisons and $k(43+42N_2)$ multiplications and $14k(N_2-1)$ exponential operators , i.e $O(kN_2)$ comparisons, $O(kN_2)$ multiplications and $O(kN_2)$ exponential operators.

m	S	Corresponding matrix	Rank	Remark
3	(1)	10 01	2	simple
	(2)	01 10	2	simple
4	(1)	10 01	2	simple
	(3)	01 10	2	simple
5	(1,2)	1100 0101 1010 0011	3	simple
	(1,3)	1010 1100 0011 0101	3	simple
	(4,2)	0101 0011 1100 1010	3	simple
	(4,3)	0011 1010 0101 1100	3	simple
6	(1)	10 01	2	simple
	(5)	01 10	2	simple

<u>Appendix</u> : Ranks of all CM types of $K = Q(\xi_m)$
$m = 3, 4, \ldots, 10$

m	S	Corresponding matrix	Rank	Remark
7	(1,2,3)	111000 010101 011001 100110 101010 000111	4	simple
	(1,2,4)	—	2	nonsimple, lifted from $(Q(\sqrt{-7}), id)$
	(1,3,5)	101010 011001 111000 000111 100110 010101	4	simple
	(1,4,5)	100110 111000 101010 010101 000111 011001	4	simple
	(6,2,3)	011001 000111 010101 101010 111000 100110	4	simple
	(6,2,4)	010101 100110 000111 111000 011001 101010	4	simple
	(6,3,5)		2	nonsimple, lifted from $(Q(\sqrt{-7}), \rho)$
	(6,4,5)	000111 101010 100110 011001 010101 111000	4	simple

m	S	Corresponding matrix	Rank	Remark
8	(1,3)		2	nonsimple, lifted from $(Q(\sqrt{-2}),id)$
	(1,5)		2	nonsimple, lifted from $(Q(i),id)$
	(7,3)		2	nonsimple, lifted from $(Q(i),\rho)$
	(7,5)		2	nonsimple, lifted from $(Q(\sqrt{-2}),\rho)$
9	(1,2,4)	111000 011001 001011 110100 100110 000111	4	simple
	(1,2,5)	110100 111000 011001 100110 000111 001011	4	simple
	(1,4,7)		2	nonsimple, lifted from $(Q(\sqrt{-3}),id)$
	(1,5,7)	100110 110100 111000 000111 001011 011001	4	simple
	(8,2,4)	000111 100110 110100 001011 011001 111000	4	simple
	(8,2,5)		2	nonsimple, lifted from $(Q(\sqrt{-3}),\rho)$

m	S	Corresponding matrix	Rank	Remark
9	(8,4,7)	001011 000111 100110 011001 111000 110100	4	simple
	(8,5,7)	000111 100110 110100 001011 011001 111000	4	simple
10	(1,3)	1100 0101 1010 0011	3	simple
	(1,7)	1010 1100 0011 0101	3	simple
	(9,3)	0101 0011 1100 1010	3	simple
	(9,7)	0011 1010 0101 1100	3	simple

References

[1] Adams,W. and Goldstein,L.J., "Introduction to number theory", Prentice-Hall Inc., New Jersey, 1976

[2] Dodson,B., "The structure of Galois groups of CM fields", Trans. of the AMS, vol 283,no 1, 1984, 1-32

[3] Fadeev,D.K., "On the divisor class group of some algebraic curves", Dokl. Tom 136 = Sov. Math, vol. 2, 1961, 67-69

[4] Greenberg,R., "On the Jacobian variety of some algebraic curves", Comp. Math., vol 42, fasc 3, 1981, 345-359

[5] Gross,B.H., "Arithmetic on elliptic curves with complex multiplication", Lectures notes in Mathematics, no 776, Springer Verlag, New York, 1980

[6] Hungerford,T., "Algebra", Springer-verlag, New York, 1984

[7] Koblitz,N. and Rohrlich,D., "Simple factors in the Jacobian of Fermat curve", Can. J. Math., vol 118, no 6, 1978, 1183-1205

[8] Kubota,T., "On the field extension by complex multiplication", Trans. of the AMS, vol 118, no ,1965, 113-122

[9] Lang,S., "Complex multiplication", Springer-Verlag, New York, 1983

[10] Murty,V.K., "Introduction to Abelian varieties", Lectures notes, Concordia University, Sept 1986

[11] ——— , "Nondegenerate CM types", Quebec Vermont number theory seminar, Technical report, Mcgill University, 1986, 59-75

[12] Ribet,K.A., "Division fields of Abelian varieties with complex multiplication", Soc. math. de France, 2^e series memoire, no 2,

1980, 75-94

[13] Serre,J.P., "Linear representations of finite groups", Springer-Verlag, New York, 1977

[14] Shimura,G. and Taniyama,Y., "Complex multiplication on Abelian varieties and its applications to number theory", Math. soc. of Japan, Tokyo, 1961